MoFo Privacy Tips for Protecting Reproductive Rights

Written by Miriam Wugmeister, Linnea Pittman, Carson Perry Martinez, and Damian Mencini. With special thanks to Jamie Levitt, Robert S. Litt, Alex Iftimie, and Margaret Eleazar-Smith. Morrison Foerster is a global technology law firm with an industry-leading privacy practice that is committed to protecting reproductive rights.

GUIDANCE FOR INDIVIDUALS

Following the Supreme Court's decision in Dobbs v. Jackson Women's Health Organization overturning Roe v. Wade, many states have banned or severely limited abortion access. In most cases, these bans prohibit people from providing abortions, but there is increasing concern about how individuals could be criminally targeted for their pregnancy outcomes. As a result, pregnant people who live in states that restrict access to reproductive health services such as abortion may want to consider how their online and offline actions might put them at risk of prosecution or in other legal jeopardy. While it is impossible to be completely anonymous when searching for and obtaining reproductive health services, individuals can take a number of steps to reduce their digital and physical footprint.

Searching for Reproductive Health Resources Online

Many organizations, from your internet service provider (ISP) to advertising companies and search engines, collect information relating to your activity on the internet. While none of the steps below will ensure you have complete privacy, there are steps you can take to limit what information is collected about you when you browse the internet. Before seeking reproductive health resources online, consider the following steps to decrease the risk of digital surveillance:

Use a Privacy Protective Browser App or Window.
These apps do not save your searches on the Internet, and thus if a law enforcement request were made to these apps to collect your search history, there would be nothing for the app to share:

- Brave Browser
- Duck Duck Go

Use Private Browsing.
If you are unable to use a privacy-protective browser, consider using private browsing settings when you are searching, which eliminates saved searches on your device. Privacy browsing does not stop ISPs like Google or Microsoft from collecting and storing information about your search history because your internet connection will not be encrypted, but it does mean that your search history will not be stored on your device. In addition to using private browsing, it is important to routinely delete your history (see Recommendation under Deleting Data After Reproductive Health Services below for more information):

- Chrome
- Firefox
- Safari
- Edge

Use a VPN.
Use a virtual private network (VPN) to protect Internet activity. VPNs mask your online activity by routing your internet connection through an encrypted server, preventing ISPs from seeing what you are doing online. That way, if your ISP receives a law enforcement request, they will not have information to hand over to law enforcement:

- Tips on choosing a VPN
- iPhone: Go to Settings > General > VPN. If you have installed one of the recommended VPNs or another VPN of your choice, it should appear here for you to select.

- Android: Go to Settings > Network & Internet > VPN. Again, if you have already downloaded one of these apps, select it and login to your account.
- Windows/Mac: Installing a VPN on a desktop or laptop computer will operate like installing any app on your device. Go to the service provider's website and download the offical app from the service. Once the download is finished, go through the installation process on screen.

Opt Out of Third-Party Tracking.
When third-party tracking is enabled, third parties like advertisers and data brokers can track you across your apps and websites on your mobile devices through an ad identifier, a string of numbers and letters that identifies your smart device (“IDFA” on iOS or “AAID” on Android), that every app can see. Third parties use the ad identifier to collect your activity and create a profile about you, which they use to send you targeted ads or sell to other companies. Opting out of tracking across third-party apps and websites on your phone will prevent third parties from seeing your ad identifier and creating that profile, making it less likely that law enforcement or third parties can obtain data from them through legal process:

- Android: Go to Settings > Google > Ads > Toggle "Opt out of ads personalization" to On. You can also reset your Advertising Identifier in both Android and iOS to unlink any previous data associated with your ID.
- iOS: Go to Settings > Privacy > Tracking > Toggle "Allow Apps to Request to Track" to Off. You can also reset your Advertising Identifier in both Android and iOS to unlink any previous data associated with your ID.

Block Targeted Advertisements.
While opting out of third-party tracking will decrease the majority of the data third parties collect about you, first parties (i.e., the actual apps installed on your phone themselves), may still collect data about you, use that data to themselves to serve you targeted ads, and capture your interaction with the ads. Opting out of targeted advertising on your browsers and social media platforms will not prevent first parties from collecting information about you completely, but it will prevent them from collecting information related to your interaction with targeted ads. Opting out may also prevent you from seeing potentially unwanted ads by anti-abortion groups:

- Privacy Badger
- Ublock Origin
- National Advertising Initiative Consumer Opt Out
- Facebook
  Browser: Go to Settings & Privacy > Settings > Ads > Ad Settings >
  - Data about your activity from partners > Toggle to Off
  - Categories used to reach you > Toggle all categories to Off
  - Ads show off of Facebook > Toggle to Not Allowed
  App: Go to Settings & Privacy > Settings > Permissions > Ad Preferences > Ad settings
- - Data about your activity from partners > Toggle to Off
  - Categories used to reach you > Toggle all categories to Off
  - Ads show off of Facebook > Toggle to Not Allowed
  You may also want to clear previous activity and disconnect future off-Facebook activity.
- Instagram: Settings > Ads > Ad Preferences > Toggle data from partners to Off
- TikTok
- Twitter: Go to Settings & Privacy > Privacy & Safety > Data sharing and off-Twitter activity
  - Ads Preferences > Unclick the box for personalized ads

- Off Twitter activity > Unclick the box for Allow use of where you see Twitter content across the web and Personalize based on your inferred identity.
- Data sharing with business partners > Unclick the box for allow additional information sharing with business partners.
- Location information > Unclick the box for personalize based on places you've been.

- Snapchat

Take Precautions when Using Menstruation Apps.
Menstruation or period-tracking applications can be used as evidence in a prosecution if law enforcement obtains data from these apps through legal process or if law enforcement determines you installed the application on your phone through a search warrant. However, they can be useful tools to avoid an unwanted pregnancy. If you choose to use these applications, take precautions. Ensure that the app of your choice engages in best practices for user security and privacy. Two features that offer significant privacy protection for users are: (1) storing data locally on your device rather than in the cloud, and (2) forgoing third-party tracking services that can access the data that users provide.

If you decide to use a menstruation app, four “privacy protective" applications you may consider are:

- Bloody Health
- Euki
- Planned Parenthood
- Periodical

Only Click on Trusted Resources and Websites.
Anti-abortion clinics may hold themselves out as crisis pregnancy centers and may spread misinformation or collect personal information or location information.

Crisis pregnancy centers (“CPCs”) are organizations with a primary aim of keeping people from having abortions. CPCs are often affiliated with religious organizations that oppose abortion. CPCs can be found in states that have abortion bans as well as those that do not. For a map that can help you identify (and avoid) CPCs, see https://crisispregnancycentermap.com/

Practice Good Digital Hygiene.
By practicing good digital hygiene, you can help prevent unwanted cyber or physical searches of your device. These actions make it harder for law enforcement to open your device if seized as part of an investigation or for hackers to break into your device and obtain your data:

- Keep Devices Updated. Configure your devices and applications for automatic software updates to protect your devices and systems against cyber threats.
- Create Unique Passwords. Strengthen passwords and avoid using the same password for multiple accounts.
- Enable Multi-Factor Authentication. Prevent bad actors from accessing your accounts remotely by adding an extra step to access accounts.

Communicating with Reproductive Health-Related Services

If a valid warrant or subpoena is served on an organization where you received reproductive health services, including abortion clinics, OB-GYN offices, hospitals, and birthing centers, the organization may be legally required to turn over sensitive information to law enforcement. Where possible, limit

the personal information that is shared with reproductive health services to only that which is necessary to obtain care. When communicating about reproductive health services, consider the following steps to enhance the privacy of your communications:

Use Secondary Numbers
Call clinics, healthcare providers, and transportation services using a secondary phone number or buy a burner phone using cash rather than using personal devices. Using a secondary phone number provides an additional layer of privacy (not *anonymity*) to your telephone records by making it more difficult for law enforcement or third parties to connect your phone number to a certain clinic's records. Distancing your phone number from the clinic's records makes it harder for police or third parties to use your phone call logs to clinics as potential evidence against you:

- Google Voice (free)
- Hushed (paid)
- Burner (paid)

Use End-to-End Encrypted Communication Apps
Use end-to-end encrypted communication apps for messages, phone calls, or video calls when communicating with clinics or healthcare providers. Consider turning on automatic message deletion where possible and turning off automatic back-ups.

- Signal
- FaceTime
- Duo
- Zoom

Create a New, Encrypted Email Address
Create an encrypted secondary email address for communicating with clinics or healthcare providers rather than using a personal email address. This may prevent the services from reading emails shared on the platform.

- Proton
- Tutanota

If a Police Officer Approaches or Contacts You

State law enforcement of abortion laws will likely depend less on whether a person turns off their Bluetooth or disables third-party cookies and more on how many people they tell, how they communicate with those people, whether they are mindful about reducing their digital footprint, and whether they have counsel. This is because state law enforcement investigations often rely on public tips, witnesses, and information provided voluntarily by the subject of the investigation, including voluntarily providing access to their cell phone. When speaking with a police officer, do not hand over your private, and potentially incriminating, information freely:

If asked to interview with the police, **do not do it without a lawyer**. You have the right not to talk to the police about anything without a lawyer, but it is up to you to assert that right.

If you have been questioned or arrested—or you think you will be questioned or arrested—by the police because of your abortion contact the **Repro Legal Helpline**. This helpline is a free and

confidential legal service. Lawyers on the helpline will work to help you find a lawyer. If you already have a lawyer, Repro Legal Helpline may be able to work with your lawyer to help defend you.

- If a police officer approaches you asking to search and/or seize your device, **ask them if they have a warrant.**
- If the officer does not have a warrant, inform the police that you do not consent to their requests.
  Do not give the police your device voluntarily, even if asked.
- If the officer does have a warrant, comply with their requests but make it known that you object and are not complying with the request voluntarily.
  Do not provide your password voluntarily, even if asked; law enforcement cannot compel you to do that.
  If you are asked to use your biometric identifiers (e.g., fingerprint or facial recognition) to open your phone, **make sure that the warrant specifically authorizes that**.
- If the warrant **does not authorize** the use of biometric identifiers, you do not need to unlock your phone. However, if the officer insists, comply rather than resist physically.
- If the warrant **does authorize** the use of biometric identifiers, comply with the warrant while making it clear to the officers that you object to being compelled to unlock your phone.
- After complying, **consider challenging the search or seizure** through a suppression motion with legal counsel.
  After law enforcement contacts you, **do not delete any data** without first consulting with legal counsel.

Obtaining Reproductive Health-Related Services

When traveling to receive, and while receiving reproductive health services, consider the following steps to increase the likelihood that your plans and movements remain private:

Be Mindful of Your Mail.
Law enforcement can examine (but not open) your mail without a search warrant. If buying abortion medications (i.e., mifepristone and misoprostol) online, consider creating a mail forwarding address in a state without restrictions on using telehealth to access abortion medications and ship your medications to that address. Seek legal advice before engaging in this activity.

- PostScan Mail
- iPostal1
- Anytime Mailbox

Shred Sensitive Documents.
Law enforcement can search your trash without a search warrant. Be careful of what you throw away (e.g., pregnancy tests), and shred any sensitive documents (e.g., insurance or reproductive health services receipts).

Think Before You Talk About It
Tell as few people as possible (and do not talk to your smart speaker or voice assistant) about your plans. If you do tell someone, tell someone you trust in person or over an encrypted call.
Do not tell people on social media.

Don’t Post About it.

Do not post online about your plans.

Proceed with Caution When Seeking Care From a Healthcare Provider in States That Are Hostile to Abortion.
Healthcare professionals may be required to report people they suspect of having had an abortion. So, if you are seeking care from a healthcare provider and you do not know whether that provider supports abortion access or whether your state law requires reporting, avoid talking about your abortion.

Avoid Ride-sharing Apps.
Do not use ride-sharing apps to go to clinics. Instead, take a taxi and pay with cash. If you must use a ride-sharing app, do not select the clinic as your destination. Use a nearby business instead.

Turn Off Location Tracking or Leave Your Devices Behind.
Only take devices you need. Before you go to a provider, put your phone on airplane mode or turn it off. When you finish your appointment, ask the clinic to call a taxi for you if you don't have your phone with you or if your phone is turned off. If your phone must be with you and turned on, turn off cell service, Wi-Fi, Bluetooth connectivity, and location services.

To turn off location services:
If you must use location services on your device, consider resetting your device's advertising ID before and after visiting sensitive locations. This will make it harder to connect such data to you.

- Android: Go to Settings > Services > Ads > Reset Advertising ID > Confirm by clicking OK.
- iOS: Go to Settings > Privacy > Advertising > Reset Advertising Identifier > Confirm by clicking Reset Identifier.

If financially practicable, consider buying a burner phone to bring with you instead.

Do Not Park Onsite.
If you drive, do not park at the clinic. Park at a nearby business location and walk to and from the clinic. Anti-abortion protestors are reported to be taking photos of cars and recording license plates upon their arrival at reproductive healthcare clinics.

If Possible, Avoid Using a Credit or Debit Card.

- Pay for lodging, transportation, services, or medicine in cash or a prepaid gift card.
- Credit card companies and financial institutions keep records of all transactions.
- Be mindful of what you are throwing away in the trash, such as any receipts/billings from a clinic or insurance company.
- Consider paying for related everyday reproductive healthcare purchases (e.g., pregnancy tests, prenatal vitamins, and menstrual products) with cash, too.
- Avoid using in-store loyalty or membership cards or online accounts when you do so.

Dress to Conceal.
Conceal yourself when you go to the clinic to prevent others from recognizing you or taking your photograph as well as security cameras from capturing footage of your movements.

Deleting Data After Reproductive Health Services

If you were unable to use encrypted browsing and email services or messaging apps when searching for or contacting reproductive health-related services, consider deleting any data potentially connected to the services you received:

Delete Browsing and Internet Histories.
Delete browsing and internet histories to decrease the likelihood that law enforcement could see your searches on your devices if they were seized or could subpoena ISPs for your search information:

- Microsoft Edge
  - Private Browsing
  - Delete Browsing History
  - Delete Cookies
- Chrome
  - Private Browsing
  - Delete Browsing Data
  - Clear Cache & Cookies
- Firefox
  - Private Browsing
  - Delete Browsing, Search, and Download History
  - Clear Cookies and Site Data
- Safari
  - Private Browsing
  - Delete your Browsing History
  - Remove stored cookies and website data
- iPhone, iPad, or iPod Touch
  - Clear history and cookies
- Google Data
  - Delete your activity

Delete Device Data and Accounts.
If you download information regarding reproductive health services on your computer or phone, consider deleting your device data. Note: this action would wipe everything from your device and/or your account (including personal items like your contacts, text message history, and family photos). If you automatically back up to iCloud, delete this back-up copy as well because law enforcement can obtain a search warrant for cloud storage accounts:

- Computers
  - Delete data on macOS
  - Delete data on Windows
- Phones
  - Delete all content and settings from iPhone
  - Factory-reset your Android phone
- Delete your google account
- Delete your Apple ID and data

Key Takeaways

Although there is no perfect solution to shield you from digital surveillance, implementing the recommendations above will greatly improve your digital privacy. Increasing your digital privacy may

involve complicated steps and create some inconveniences to everyday use of your devices by impairing device performance or removing some device features. Nevertheless, these difficulties are certainly worthwhile when considering the alternative—potential prosecution. If you are only able to implement a few measures, consider the following key steps:

1. **Think before you talk about it.**
   The fewer people who know, the fewer people there will be to report it.
2. **Don’t write about it.**
   Text messages, posts, and online searches can be critical evidence.
3. **If you write about it or talk about it, do it securely.**
   FaceTime and Duo, the default video calling applications on iOS and Android, are both end-to-end encrypted and offer convenient ways to communicate securely (without writing things down).
4. **Browse privately and delete your data.**
   Browsing or searching the internet securely only takes a couple of clicks and can greatly improve your digital privacy. Routinely deleting your search histories and location histories provides an additional layer of security.
5. **Call a lawyer.**
   If a law enforcement officer approaches you, exercise your constitutional right to call a lawyer and seek legal advice.

GUIDANCE FOR CLINICS AND HEALTHCARE PROVIDERS

Following the Supreme Court's decision in Dobbs v. Jackson Women's Health Organization overturning Roe v. Wade, many states have banned or severely limited abortion access. As healthcare providers adapt to this new reality, healthcare providers offering reproductive health services, particularly in states that have banned or severely restricted abortion, must now consider whether and how their data collection and retention practices may put their patients at risk of potential prosecution.

While it is impossible to avoid collecting any sensitive data in the process of providing reproductive health-related care to patients, healthcare providers offering reproductive health services can take steps to mitigate the risks associated with the data they collect, maintain, and disclose.

When Collecting and Processing Patient Data

Clinics and healthcare providers may wish to minimize the amount of information they collect. For the information they must collect, clinics and healthcare providers should work to keep patient information as private as possible. Consider these steps:

Employ Data Minimization Techniques.
Take inventory of the information you currently collect about patients. Only collect information that is absolutely necessary to carry out reproductive health services.

Do not capture specific appointment types (e.g., visit, procedure, consultation, check up) where possible.

- List all appointments as "appointments" so if law enforcement requests data, the response would include "appointment" with no information about the type of procedure or consultation performed.
- If clinics have their own communications system with patients, the contents of the communications can only be released with a warrant or court order.

Note: Hospitals, facilities, and physicians providing abortion-related services may submit regular reports regarding the facility at which the abortion was performed, the physician performing the procedure, the patient's demographic characteristics, gestational age, and the abortion procedure used, among other state-specific requirements.

Use a VPN.
Use a virtual private network (VPN) for all business activity. VPNs mask your employees' activity by routing their internet connection through an encrypted server, preventing ISPs from seeing what employees are doing online. That way, if your ISP receives a law enforcement request, they would have limited information to hand over to law enforcement:

Tips on Choosing a VPN

- Install a VPN on iPhone
  Go to Settings > General > VPN. If you have installed one of the recommended VPNs or another VPN of your choice, it should appear here for you to select.
- Install a VPN on Android
  Go to Settings > Network & Internet > VPN. Again, if you have already downloaded one of these apps, select it and login to your account.

- Install a VPN on a PC
  Installing a VPN on a desktop or laptop computer will operate like installing any app on your device. Go to the service provider's website and download the offical app from the service. Once the download is finished, go through the installation process on screen.

Block Ads from Websites.
A number of healthcare providers have inadvertently included advertising pixels both on their websites and within protected portals that have revealed sensitive personal information. Make sure websites that collect URLs associated with searches or appointments do not have advertising pixels. This will prevent your website from revealing the identity of visitors (i.e., potential patients) to ad brokers.

Create a Data Deletion Protocol.
Have short data retention policies and securely dispose of or de-identify data when it is no longer needed (note that state laws may impose retention requirements). Create secure disposal procedures for any physical papers with patient information.

Recommend that Patients Avoid Using Credit and Debit Cards to Pay for Appointments.
When patients book an appointment, consider recommending that they use a form of payment that is not identifiable, such as cash or a gift card. This can help your patients minimize their risk.

Make Appointments Securely.
Use secure appointment booking software (if available) or book appointments with encrypted email services or messaging applications. This would prevent the app from reading messages shared on the platform, but encrypted messages could still be accessed by law enforcement with a search warrant if the messages are retained on devices. Consider turning on automatic message deletion where possible and turning off automatic back-ups.

- Encrypted Email
  - Proton
  - Tutanota
- Encrypted Messaging
  - Signal
  - Signal for iOS
  - Signal for Android
  - Set and manage disappearing messages
- Encrypted Videoing
  - Duo
  - FaceTime
  - Zoom

When Responding to Legal Process

Upon receiving a request for patient information from law enforcement, review the request for compliance with the Health Information Portability and Accountability Act (HIPAA) and other legal requirements and respond appropriately. Consider these steps:

1. **Always Engage with Legal Counsel.**
   If possible, have legal counsel ready so you are prepared and can act swiftly if law enforcement contacts you.
2. **Ask for Valid Legal Process. Only provide data in response to valid legal process (i.e., a subpoena, court order, or search warrant).**
   - If law enforcement requests information or records, ask that they return with valid legal process.
   - Absent a valid legal process, disclosure is not permitted under HIPAA and fines may be imposed.
   - For additional information, see HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care.
3. **Consider Potential Objections. Consider whether a reasonable ground for objection exists (consult with an attorney about this):**
   Did the correct court issue the request?
   - Subpoenas, orders, and warrants issued across state lines are generally unenforceable; the request must be issued by a court within the state in which the provider or insurance company has a business presence.
   - If the court does not have jurisdiction, you are not obligated to comply.
   Is the warrant or subpoena particularized?
   - Are accounts/individuals specified?
   - Is there a limiting time frame?
   - Law enforcement cannot, in most cases, broadly ask for "all patients" who visited within a particular timeframe. Instead, requests for data must be specific and limited to individual patients (or a handful of patients if there was evidence they were acting together).
4. **Review Requests. If you receive a subpoena, court order, or warrant, consider whether the HIPAA rules are met, or, if there is a conflict between state law and HIPAA, consider whether the law that provides the greater protection applies.**
   For court orders, warrants, and subpoenas issued by a judicial officer or grand jury subpoena, HIPAA permits covered entities to disclose the requested information.
   For administrative subpoenas, HIPAA permits disclosure if:
   - The information sought is relevant and material to the legitimate law enforcement inquiry;
   - The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
   - De-identified data could not be reasonably used.
   For subpoenas not accompanied by an order of a court or administrative tribunal, HIPAA permits disclosure if:
   - There is written satisfactory assurance from the requesting agency that they made a good-faith effort to notify the patient of the subpoena, gave the patient a chance to object, and the objection has either been declined or time has elapsed;
   - There is a protective order requested or in place; or
   - The covered entity has made reasonable efforts to contact the patient about the subpoena.
5. **Respond to the Request. Petition the court if you decline to provide information.**
   Failure to respond to a valid order, warrant, or subpoena may result in fines or penalties.
6. **Only Disclose Requested Information. If HIPAA and/or state requirements are met and there are no grounds for objection, disclose only the PHI expressly requested by the legal request (i.e., the "minimum necessary" to comply with the request).**
   - Information not specifically requested should be redacted or not shared.
   - It may violate HIPAA to share such unrequested records.

7. **Only Disclose at the Specified Time.**
   If the subpoena requires disclosure at a specific time, do not disclose information before the deadline without the patient's consent. Doing so may deprive the patient of the opportunity to seek to quash the subpoena.
8. **Notify Patients. Where possible, notify patients whose data has been released in response to a valid legal request.**
   - Warrants may come with a gag order preventing notification. Consult with legal counsel if considering contesting a gag order.
   - Subpoenas may impose state law-specific non-disclosure requirements.
9. **Consider State Laws. Determine whether state law provides any guidance. See for example, Connecticut's "Reproductive Freedom Defense Act," which**
   - Prevents HIPAA-covered entities from disclosing PHI related to reproductive health services without the written consent of the patient;
   - Prohibits out-of-state judicial requests to issue a subpoena in Connecticut seeking to collect reproductive health PHI; and
   - Prevents public agencies from aiding investigations seeking to impose criminal or civil liability for reproductive health care.

RECOMMENDATIONS FOR TECHNOLOGY COMPANIES

If law enforcement is going to serve legal process on a private entity in a reproductive health case, it is most likely going to be on a major technology company under the Stored Communications Act (SCA) because: (1) these companies have broad data holdings on individuals, and (2) law enforcement is often most familiar with serving SCA legal process on these companies.

While major technology companies must comply with SCA requests, they may wish to consider taking the additional steps to enhance privacy for reproductive rights listed below.

1. MINIMIZE COLLECTION OF SEARCH AND LOCATION DATA RELATED TO SENSITIVE MEDICAL FACILITIES.

Technology companies may wish to limit the collection of search and location data related to sensitive medical facilities. For example, on July 1, 2022, Google announced that it will automatically delete location data for individuals whose data shows they visited a counseling center, abortion clinic, fertility center, or similar medical center. Search engines may expand this approach to automatically delete search terms for individuals researching these facilities.

2. PROVIDE ADDITIONAL PROTECTIONS AND DATA MINIMIZATION PROCEDURES FOR SENSITIVE HEALTH DATA.

Technology companies may wish to provide end-to-end encryption for health data collected from devices and third parties, or consider automatically deleting health histories related to reproductive health.

3. DO NOT IDENTIFY PREGNANT PEOPLE THROUGH CONSUMER TRACKING TOOLS.

Technology companies that are able to identify pregnant people through purchases, searches, or other online activity may wish to stop specific targeted advertising based on a person’s pregnancy, birth control needs, or reproductive health inquiries.